J Med Syst (2018) 42:130
https://doi.org/10.1007/s10916-018-0982-x

MOBILE & WIRELESS HEALTH

Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring

Kristen N. Griggs[1] · Olya Ossipova[1] · Christopher P. Kohlios[1] · Alessandro N. Baccarini[1] · Emily A. Howson[1] · Thaier Hayajneh[1]

Received: 21 March 2018 / Accepted: 18 May 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract

As Internet of Things (IoT) devices and other remote patient monitoring systems increase in popularity, security concerns about the transfer and logging of data transactions arise. In order to handle the protected health information (PHI) generated by these devices, we propose utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, we created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner.

Keywords Blockchain · IoT · Healthcare · Smart contracts · Secure remote patient monitoring · Ethereum · PHI · WBAN · HIPAA

Introduction

The rapid growth of Internet of Things (IoT) devices and wearable technology has opened up new possibilities in the realm of medical sensors, particularly for remote patient monitoring. One subset of this IoT healthcare trend is Wireless Body Area Networks (WBANs). In a WBAN, a patient is equipped with various wearable or implanted medical devices that take real-time measurements of vital indicators, such as heart rates or glucose levels. Other devices may act as actuators, which can provide automated treatments based on the measurements taken by the sensors. All of the patient's WBAN devices report to a master device (typically a mobile phone) which transmits the collected data to healthcare providers and provides an interactive interface for the user. This remote monitoring reduces the need for time-consuming doctor's appointments and allows patients to go about their daily lives more freely [3].

The popularity of remote patient monitoring is rapidly growing; in 2016, 7.1 million patients around the world utilized remote monitoring as part of their health management, and the number is predicted to reach 50.2 million by 2021 [12]. Additionally, the U.S. Centers for Medicare & Medicaid Services implemented new reimbursement incentives as of January 1, 2018 that promote the use of devices with an "active feedback loop" to provide real-time monitoring [7].

As the realm of remote patient monitoring expands, concerns about efficient and secure transmission of the medical data are raised. The measurements collected

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ Thaier Hayajneh
thayajneh@fordham.edu

Kristen N. Griggs
kgriggs2@fordham.edu

Olya Ossipova
oossipova@fordham.edu

Christopher P. Kohlios
ckohlios@fordham.edu

Alessandro N. Baccarini
abaccarini@fordham.edu

Emily A. Howson
ehowson@fordham.edu

[1] Fordham Center for Cybersecurity, Fordham University, New York, USA

Published online: 06 June 2018

from different sensor devices - which may have different manufacturers - must be aggregated, formatted, and processed together in order to provide integrated health management. However, healthcare data is a lucrative target for hackers, and there is a strong motivation in government regulation to secure protected health information (PHI) transmission. Thus, patient privacy must be preserved, yet the data in electronic health records (EHRs) must be easily manageable and transferable. Furthermore, commands issued to actuator nodes inside of the IoT devices must also be securely logged as both a treatment for the patient and a record of who permitted it, in order to protect the integrity of the patient's care and maintain an accurate timeline of events. To address these concerns, we propose integrating WBAN systems with smart contracts on a consortium-managed blockchain in order to provide a distributed data processing service that creates an immutable log of the transactions between the WBAN devices and the healthcare providers. With this system, having an immutable ledger and automatic notifications of health events in a secure manner will offer patients peace of mind when it comes to wearing medical devices. Secure remote monitoring provides medical professionals real-time notifications about their patients, thus propagating the practice of precision medicine. The automation of health notifications from multiple devices via a single system using smart contracts is a revolutionary approach that allows healthcare providers to easily integrate new medical technology. Figure 1 illustrates the basic design of our system.

Blockchain technology, as initially proposed by Satoshi Nakamoto [14], is the basis for smart contracts. It acts as a shared decentralized ledger to record transactions. There are three types of blockchains: public, private, and consortium. A public blockchain is predominantly used to decentralize networks and offer secure transparency. In contrast, private and consortium (semi-private) blockchains are preferred when more control and privacy are required. Our system utilizes a consortium blockchain due to the cost and increased privacy for PHI. A key reason for using blockchain technology in our system is its features of consensus and decentralization. Blockchain provides security because it is based on the idea of a lack of trust (i.e. through algorithms such as proof-of-work or Practical Byzantine Fault Tolerance) and utilizes the consensus or agreement of nodes to authorize the additions of blocks to the chain, which acts as a general ledger for all transactions.

Blockchain technology has aided in the advancement and effectiveness of many industries. It can be used to record the events a product or subject experiences from its origin to the current state in an unalterable log. Use cases include checking the freshness of groceries, the authenticity of a specific piece of art, or the ownership of a piece of land. Blockchains are also capable of implementing smart contracts, which are pieces of code that can automatically execute based on predefined conditional triggers. Our system utilizes these contracts to facilitate automatic analysis of health data collected by the WBAN devices based on custom threshold values for each patient, which can trigger alerts for unusual activity. In addition to supporting the smart contracts, our proposed blockchain would keep a permanent log of the sequence of transmissions to and from a WBAN node in order to track metadata about measurements taken and treatment commands issued.

When dealing with PHI, privacy and authenticity are essential. This system utilizes the distributed ledger properties of blockchain for authenticity and verifiability, while maintaining privacy through permissioned consortium management and anonymized accounts. Only authorized entities can access the blockchain for inspection and block verification, in contrast to a public blockchain like Bitcoin. Each

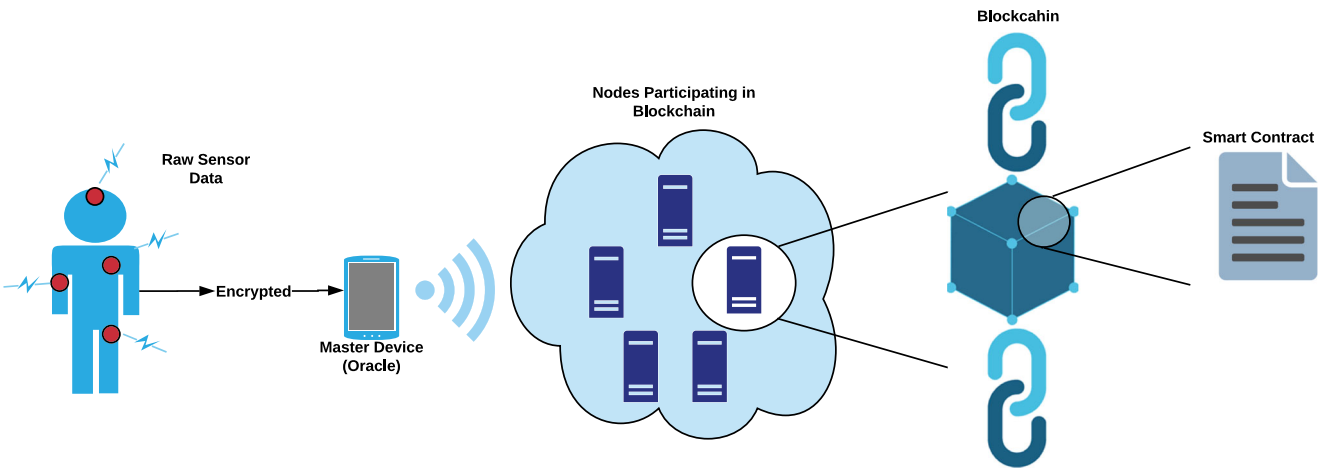

Fig. 1 Raw sensor data is aggregated by the master device and then sent to nodes in the blockchain for processing by the smart contract

authorized user will also have their own anonymous account that can only be traced by their own discretion. This promotes transparency for patients and allows them to better manage their own healthcare data.

The paper is outlined as follows: "Related work" of this paper will discuss the existing literature related to this topic. Section "System design" outlines the system we have proposed, while "Implementation" will cover our smart contract implementation. Section "System analysis" will contain an overarching analysis of our system, including a comparison to the traditional system ("Comparison to traditional systems"), a security analysis ("Security analysis"), and its limitations ("Limitations"). Section "Conclusion and future work" concludes the paper and discusses future work.

Related work

Though several papers provide plausible applications of blockchain in healthcare [8, 9, 16, 18], at the time of writing, no comparable research or publicly available software following our proposed method was found. Larger corporations, such as IBM with its project Hyperledger, have marketed a capability to apply blockchain to healthcare and IoT [16]. However, we could not find any publications referencing their operational model. Remote Patient Monitoring (RPM) research is currently focused on the improvement of patient outcomes [15] and wireless network sensors [10] [1] as opposed to the application of blockchain technology to RPM. Other interesting proposals include utilizing out-of-band authentication schemes for Internet of Things (IoT) devices [17].

However, the largest focus has been applying blockchain to EHRs to facilitate interoperability. MIT has released a prototype called Medrec, which is a practical way to share healthcare data between EHRs via blockchain [9]. Alternatively, people are exploring developing an EHR with blockchain as the core infrastructure, meaning any data stored in said EHR will be recorded in a block. A good example of this is the ICO for Medical Chain, a company working on developing the first EHR based on blockchain to place the ownership of PHI into the hands of the patient, as opposed to a myriad of doctors and medical facilities [13]. The trend in healthcare is toward patient-controlled access. Yue et. al. developed a concept for an application that gives patients the ability to grant access to information about their health records (stored on a blockchain) to designated individuals [18]. Our system will also incorporate a patient centric approach, allowing multiple IoT devices to be linked to one patient. However, the issue with [13, 18] lies the in size of the blocks. A block on a blockchain is meant to store transactions that are short statements for record keeping. Putting entire health records onto a blockchain would greatly inflate the size of the entire chain, which would then require much more storage at each node.

Thus, in the field of healthcare technology, there are many proposed adaptations of blockchain, none of which are completely comparable to ours. As such, we anticipate a high adaptability of our blockchain-based system in the field of healthcare.

System design

We outline the system as follows. A patient remotely monitored by a doctor is equipped with various medical devices, such as an insulin pump or blood pressure monitor. The raw data is sent to a master "smart device," typically a smartphone or tablet, for aggregation and formatting by the application. Once complete, the formatted information is sent to the relevant smart contract for full analysis along with customized threshold values (Fig. 1). In the Ethereum protocol, the source for the information fed to the smart contracts is known as the "Oracle" [6]. In this case, the Oracle is the smart device, which communicates directly to the smart contracts. The smart contract will then evaluate the provided data and issue alerts to both the patient and healthcare provider, as well as automated treatment instructions for the actuator nodes if desired (Fig. 2).

No confidential medical information will be stored on the blockchain or in the smart contracts because of HIPAA compliance reasons. We are only recording the fact that events occurred and using the blockchain technology as a ledger. The measurements themselves will be forwarded to a designated EHR storage database, while a new transaction will be added to the blockchain stating that the data was successfully processed. The system will integrate with EHR APIs and send data directly to the EHR for storage. Similarly, all treatment commands from the smart contract and healthcare provider will be recorded as complete in a blockchain transaction. These blockchain transactions can then be linked to the EHR in order to provide authentication of the data in the patient's medical history as a comprehensive record of care. This authentication will help to prevent and detect alterations of a patient's EHR, whether it be on purpose or accidental.

This system will have a private and consortium-led blockchain, meaning that only authorized viewers can read the blocks and only designated nodes can execute smart contracts and verify new blocks. Limiting the viewers to only invested parties such as care providers, device manufacturers, and patients themselves will help to reduce excess exposure of information by requiring authentication to access the application. In the consortium style of blockchain management, a set of pre-approved members

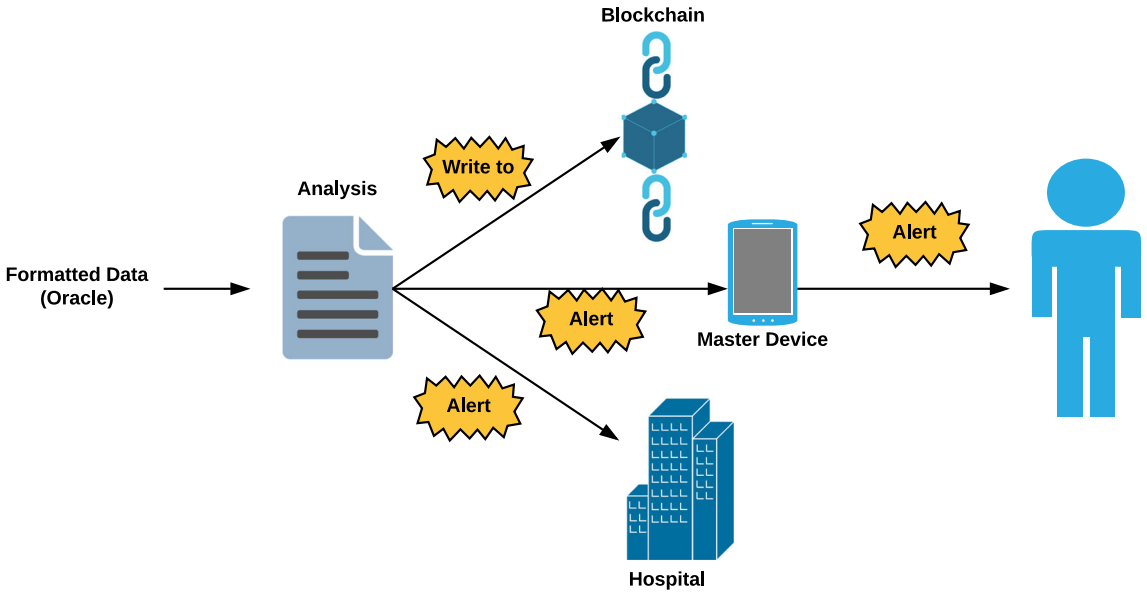

Fig. 2 Formatted data from the smart device is sent to the smart contract, which processes and performs necessary actions based on the results and predetermined parameters

operate the nodes in the blockchain, and a valid block must contain signatures from a minimum number of members (i.e. 10 out of 15). This framework would allow different healthcare companies to participate in the system while still maintaining a measure of decentralized management. Additionally, by using only pre-authorized verification (mining) nodes, it will ensure that no rogue nodes could collude to insert false transactions into the chain, as well as eliminating the need to pay currency for proof-of-work. Instead, protocols such as Practical Byzantine Fault Tolerance (PBFT) can be utilized to achieve consensus since the participating nodes are known and vetted [5].

The smart contracts themselves will be modular and customizable for each patient and their devices. The structure will be tiered, with all master devices calling the same initial smart contract, which will in turn call the relevant sub-contract for the specific patient's device and pass it the input data and custom threshold values. This individual contract will analyze the data according to the threshold values, and then issue any necessary alerts or treatment commands based on its findings. A contract cannot be edited after deployment, but rather must be "killed" and a new contract issued, so this modular structure makes it easy to replace a device's contract without affecting the operation of others.

Implementation

As a proof-of-concept, we implemented smart contracts using the Ethereum coding language Solidity. It is important to note that we are not running our operations and smart contracts on the public Ethereum blockchain, but on a separate, private chain using Ethereum's protocol. This provides the freedom to experiment outside the set parameters of the Ethereum blockchain and eliminates the need to spend Ether. Figure 3 illustrates the logic flow our smart contracts were designed to handle.

The user interface (UI) will be managed by a Decentralized Application (DApp) on the smart devices, which will be responsible for communicating with the smart contracts on the blockchain and managing user profiles. The profiles will have settings to adjust, based on their current health status. Doctors will have special administrator access to their patients' accounts, such as changing threshold values that are to be monitored. The incoming information from the sensors will be aggregated and formatted in the back-end of the DAPP and forwarded to the smart contracts, which are connected using a `web3.js` object.

For implementation in Solidity, we coded our smart contracts using Remix, a website that has a compiler to test contract functionality. However, our project is not confined to the Ethereum protocol. For an IBM Hyperledger implementation, one could use the online playground to test out a fake business network [4]. Compared to the Ethereum platform, Hyperledger is more user friendly with a UI and customer support. However, there is a monthly membership fee as an added cost. The Ethereum platform is free to use and implement, but needs a team of experts to manage it correctly.

In our system, there will be a main smart contract, `HealthContractCaller`, that the smart device will

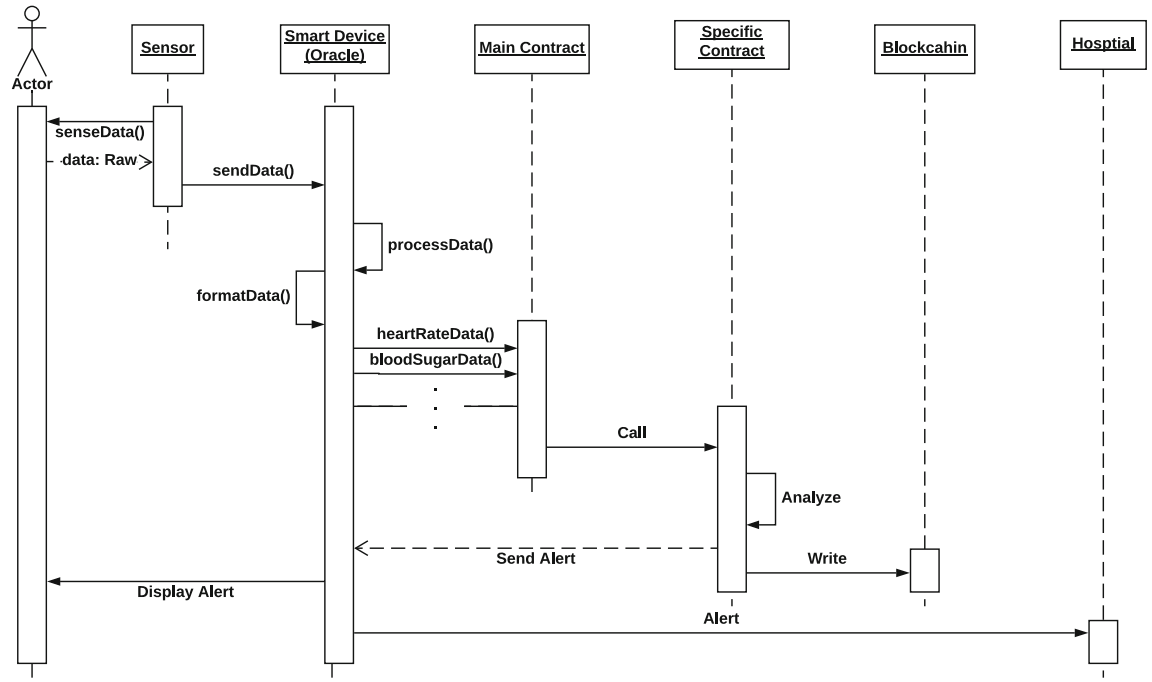

Fig. 3 The logical executon flow of the system. Sensor data is sent to the smart device, which performs the `processData()` and `formatData()` functions. The results are sent to the main contract, which is then passed to the patient's specific contract for analysis. If the measured data is outside the predetermined thresholds, necessary alerts will be triggered and a transaction will be written to the blockchain

call to handle all data. Next, `HealthContractCaller` will create the appropriate individual contract for the specific device it's receiving data from.

For example, if receiving heart rate data, the smart device will call `HealthContractCaller.heartRateMonitor()`. This will call an object of the `HealthContractCaller` and the function `heartRateMonitor()`. The smart device will pass the data and the min/max threshold values as parameters. The function will then create a new `HeartRateMonitor` object and pass the same parameters to its `analyze()` function. The two specific subcontracts will analyze the incoming data and perform the necessary response actions themselves, rather than returning control to the main contract, which functions more as a "directory" that links all devices to their relevant subcontracts for modularity and easier maintenance. If the analysis returns any code other than "OK" `(0)`, the subcontract will write this transaction on the blockchain. The same code will be sent to the smart device to either alert the user, alert the hospital, or carry out an action (e.g. pump insulin, give medicine for high blood pressure).

For the sake of simplicity, we include our three demo contracts in one file on GitHub [11]. However, for modularity and easy replacement, the contracts should be separated into different files and deployed separately on the blockchain, calling each other by their addresses.

System analysis

Comparison to traditional systems

Blockchain is a relatively recent development, and applications such as our proposed system are quite different from existing systems serving similar functions. In Table 1, we provide a side-by-side comparison of features offered by our proposed blockchain-based system and a remote patient monitoring system that relies solely on more traditional communication and data storage methods, such as cloud computing and relational databases.

Security analysis

For the sake of simplicity, we assume that all cloud and IP protocols are secure using encryption, and we do not add any more. Within the smart device, authentication must be present for the parties that could possibly be using the data (i.e. patients have the right to view but not edit their own data, while healthcare professionals have the right to edit the thresholds of their patients for the smart contracts).

The proposed consortium blockchain makes it necessary to reach a majority of signatures from consortium members to make a block valid, preventing one party from manipulating the ledger. Viewing privileges of the blockchain itself are restricted to only authorized parties (patients, caregivers,

Table 1 Comparison table between traditional systems and our proposed system

	Traditional systems	Our system
Confidentiality	Encrypted end-to-end data transmission to a designated database.	Equivalent level of security.
Availability	Database backups must be manually managed, and redundancy must be introduced to ensure service in case of failures.	We provide higher fault tolerance and service availability, as all nodes have a copy of the blockchain with every recorded transaction. Failures of one or more nodes can be managed by algorithms like PBFT.
Immutability	Databases are vulnerable to both accidental and malicious manipulation.	Verified blocks are immutable and resilient to all types of manipulation.
Traceability	Health records and logs can be changed, and detection may not be guaranteed.	Blockchain transactions can be traced from origin of creation with guaranteed immutability and are signed by the verifiers.
Speed	Transactions are limited only by network transmission speeds.	A negligible delay may occur subject to the amount of time it takes to verify a block.
Privacy	Transmissions are protected by encryption to hide any identifying information, which may still be traced back to the end users.	Anonymous addresses will protect the identity of patients, hence no associations can be made between patients and their data.
Transparency	Patients don't have direct control over their own data and cannot correlate remote transactions to their records.	Patients are able to link remote monitoring actions directly to their medical records while maintaining privacy and control.

etc). Second, no sensitive patient data is stored directly on the blockchain. The blockchain ledger storing the transactions also serves as a separate form of security for both the patient and the healthcare professional, as its detailed record could be useful for settling disputes and tracking procedures.

The electronic transmission of data falls under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996, or HIPAA. The most obvious aspect of the law that pertains to this system is the fact that data is not covered under HIPAA if it cannot be identified as belonging to a specific patient. As proposed, the data on the blockchain contains only information about transactions, and not sensitive health data. Furthermore, the patients are anonymized by the account addresses, so information is not easily linked to a specific person, thus making it permissible under HIPAA [2].

The Privacy Rule states that disclosure of personal data can only be to individuals on request or to the Department of Health and Human Services (HHS) in cases of investigation or enforcement action [2]. Another benefit of our system is that it provides authenticated and immutable records of a patient's monitoring for HHS to use for settling disputes or investigating. Our system is HIPAA compliant because it takes reasonable safeguards to secure and provide tiered access to PHI.

Limitations

As with any complex distributed system, the largest challenge is maintaining security at every individual node. As currently proposed, transmission between the patient's smart device and the blockchain nodes is over a possibly open channel (a patient's local wifi, for instance), and relies on standard channel encryption. On a large scale, however, key management may become an issue when there are many smart devices broadcasting their transactions to multiple nodes waiting to verify the next block. This could be resolved with a key management system designed to manage large numbers of keys.

An important aspect of any healthcare system is the necessity for real-time data to be accumulated and acted upon. Block verification times can be manipulated, but will still introduce some minor delay.

As proposed, the smart device collects and aggregates data from the sensor at small intervals, but sends the aggregated data in larger time intervals. The limitation here rests in perfecting the timing of the transmissions. Decisions must be made on a patient-by-patient basis, depending on the severity of the condition as well as the type of sensor they are using. It is important that this system, with current constraints, not be used for emergency response, as the delay might increase response time.

In a consortium-style blockchain that uses a consensus method such as PBFT, some human-based verification must occur before a new node is added to the system in order to prevent the presence of rogue miners. Furthermore, there must be a sufficient number of nodes online at any time in order to meet the requirements for providing the minimum number of validation signatures and maintaining the integrity of the consensus algorithm. In PBFT, this

typically means at most $(N-1)/3$ of the total nodes can be down at once, with N nodes overall [5].

As far as limitations, it is also important to note that this is an open research topic, and some of these limitations may be overcome with future development.

Conclusion and future work

In order to address security concerns about the transfer and logging of data transactions in an IoT healthcare system, we proposed utilizing blockchain-based smart contracts to perform real-time analysis and log transaction metadata for medical sensors in a WBAN. Our system would utilize a permissioned, consortium-managed blockchain to execute smart contracts that would evaluate information collected by a patient's IoT healthcare devices based on customized threshold values. The smart contracts would trigger alerts for the patient and healthcare providers as appropriate, as well as recording details about the transaction on the blockchain for verification of EHRs. As a proof-of-concept, we coded smart contracts in Solidity to demonstrate the flow of data in the system.

Blockchain has the potential to improve security in remote patient monitoring systems and automate the delivery of health-related notifications in a HIPAA compliant manner. It can fix current problems with poorly managed patient data by adding formatted and clean data to EHRs and healthcare data lakes, allowing healthcare to utilize big data with more reliable information, leading to more significant results. Future work in this area includes exploring implementation options with Hyperledger, as well as further improving the privacy of patients by introducing anonymizers that would increase the difficulty of linking transactions together.

Compliance with Ethical Standards

Conflict of interests K. Griggs declares that she has no conflict of interest. O. Ossipova declares that she has no conflict of interest. C. Kohlios declares that he has no conflict of interest. A. Baccarini declares that he has no conflict of interest. E. Howson declares that she has no conflict of interest. T. Hayajneh declares that he has no conflict of interest. This article does not contain any studies with human participants performed by any of the authors.

References

1. Almashaqbeh, G., Hayajneh, T., Vasilakos, A. V., and Mohd, B. J., Qos-aware health monitoring system using cloud-based wbans. *J. Med. Syst.* 38(10):121, 2014.
2. Assistance, H. C., Summary of the hipaa privacy rule, 2003.
3. Bolduc, M., The future of medical wearables, 2017.
4. Cachin, C., Architecture of the hyperledger blockchain fabric. In: *Workshop on distributed cryptocurrencies and consensus ledgers*, 2016.
5. Castro, M., and Liskov, B., Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst. (TOCS)* 20(4):398–461, 2002.
6. Consensys, A visit to the oracle. https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f, 2016.
7. Daniel, J. G., and Uppaluru, M., New reimbursement for remote patient monitoring and telemedicine. https://www.cmhealthlaw.com/2017/11/new-reimbursement-for-remote-patient-monitoring-and-telemedicine/, 2017.
8. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., and Wang, F., Secure and trustable electronic medical records sharing using blockchain. arXiv:1709.06528, 2017.
9. Ekblaw, A., Azaria, A., Halamka, J. D., and Lippman, A., A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data. In: *Proceedings of IEEE Open & Big Data Conference*, Vol. 13, p. 13, 2016.
10. Hayajneh, T., Mohd, B. J., Imran, M., Almashaqbeh, G., and Vasilakos, A. V., Secure authentication for remote patient monitoring with wireless medical sensor networks. *Sensors* 16(4):424, 2016.
11. Kohlios, C. P., Healthcare_iot_blockchain github.com/ckohlios/-Healthcare_IoT_Blockchain, 2018.
12. Mack, H., Remote patient monitoring market grew by 44 percent in 2016, report says. http://www.mobihealthnews.com/content/remote-patient-monitoring-market-grew-44-percent-2016-report-says, 2017.
13. Medicalchain, Medicalchain whitepaper 2.1. Tech. rep. Medicalchain, 2018.
14. Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, 2008.
15. Noah, B., Keller, M. S., Mosadeghi, S., Stein, L., Johl, S., Delshad, S., Tashjian, V. C., Lew, D., Kwan, J. T., Jusufagic, A., and et al., Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials. *npj Digital Medicine* 1(1):2, 2018.
16. Unleashed, I. B., Blockchain is good for your health, and your business. https://www.ibm.com/blogs/blockchain/2017/12/blockchain-good-health-business/, 2017.
17. Wu, L., Du, X., Wang, W., and Lin, B., An out-of-band authentication scheme for internet of things using blockchain technology, 2017.
18. Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W., Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* 40(10):218, 2016.